バイリンガルサイバーセキュリティテクニカルアーキテクト(AWSクラウドデジタルプラットフォーム開発)

Cyber Security Technical Architect

Job Information

Hiring Company
Quest Global Japan Corporation

Job ID
1602649

Industry
Software

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards, Chuo-ku

Salary
Negotiable, based on experience ~ 12 million yen

Work Hours
会社の規定に準ずる / In accordance with company regulations

Holidays
完全週休二日制（土日祝）/ 2-day weekend system (Sat, Sun, Holidays)

Refreshed
November 5th, 2026 12:00

General Requirements

Minimum Experience Level
Over 10 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Business Level

Minimum Education Level
High-School

Visa Status
Permission to work in Japan required

Job Description

≪募集要項・本ポジションの魅力 / Job Description & Position Highlights≫

- AWSクラウド基盤のサイバーセキュリティ設計やDevSecOps推進、リスク評価まで幅広く担当
- AWSやゼロトラスト、DevSecOpsなど先端技術を活用し、高度なセキュリティアーキテクトとして活躍できる
- 日本とグローバルチームをつなぐ技術的な橋渡し役として、提案力やリーダーシップを発揮できる
- 年間休日120日以上の土日祝休み、オンライン研修や充実した福利厚生で長期的に働きやすい

- You'll be responsible for a wide range of tasks, from designing cybersecurity for AWS cloud infrastructure to

promoting DevSecOps and conducting risk assessments.
- You'll have the opportunity to work as a senior security architect, leveraging cutting-edge technologies such as AWS, Zero Trust, and DevSecOps.
- You'll serve as a technical liaison between Japanese and global teams, demonstrating your proposal skills and leadership.
- With over 120 days off per year—including weekends and holidays—as well as online training and comprehensive benefits, this is a great environment for long-term employment.

【業務内容 / Responsibilities】

- AWSクラウドベースのデジタルプラットフォームおよびエンタープライズアプリケーション向けのサイバーセキュリティアーキテクチャ設計をリードする
- AWS環境におけるセキュアなクラウドアーキテクチャ、ネットワークセキュリティ、IAM戦略、暗号化、ログ管理、監視、およびコンプライアンス制御を定義・実装する
- 顧客のエンジニアリング、インフラ、DevOps、およびアプリケーション開発チームと連携し、SDLC全体にセキュリティを組み込む
- クラウドネイティブアプリケーションおよびマイクロサービスに対するセキュリティリスク評価、脅威モデリング、脆弱性分析、およびセキュリティレビューを実施する
- クラウドセキュリティのベストプラクティス、ガバナンスポリシー、およびセキュアコーディングガイドラインを策定・推進する
- IAM、GuardDuty、Security Hub、WAF、Shield、CloudTrail、KMS、InspectorなどのAWSネイティブセキュリティサービスを活用したセキュリティソリューションを設計・支援する
- DevSecOpsパイプライン、コンテナセキュリティ、CI/CDセキュリティ、およびKubernetes/EKSセキュリティ対策の実装を支援する
- 日本側ステークホルダーとのアーキテクチャ検討、顧客会議、および技術提案活動に参画する
- セキュリティインシデントを分析し、対策案の提示および根本原因調査を支援する
- サイバーセキュリティ標準、データ保護要件、および業界規制への準拠を確保する
- オンサイト顧客チームとオフショア / グローバル開発チーム間の技術的なブリッジ役を担う
- アーキテクチャ文書、セキュリティ設計書、運用ガイドライン、および技術レポートを作成する。

- Lead cybersecurity architecture and security design activities for AWS cloud-based digital platforms and enterprise applications
- Define and implement secure cloud architecture, network security, IAM strategy, encryption, logging, monitoring, and compliance controls in AWS environments
- Collaborate with customer engineering, infrastructure, DevOps, and application development teams to ensure security is integrated throughout the SDLC
- Conduct security risk assessments, threat modeling, vulnerability analysis, and security reviews for cloud-native applications and microservices
- Establish and enforce cloud security best practices, governance policies, and secure coding guidelines
- Design and support security solutions using AWS native security services such as IAM, GuardDuty, Security Hub, WAF, Shield, CloudTrail, KMS, and Inspector
- Support implementation of DevSecOps pipelines, container security, CI/CD security, and Kubernetes/EKS security measures
- Participate in architecture discussions, customer meetings, and technical proposal activities with Japanese stakeholders
- Analyze security incidents, provide mitigation strategies, and support root cause investigations
- Ensure compliance with cybersecurity standards, data protection requirements, and industry regulations
- Act as a technical bridge between onsite customer teams and offshore/global engineering teams
- Prepare architecture documents, security design specifications, operational guidelines, and technical reports

■募集背景 / Background of the Recruitment：
当社は、戦略的な医療デジタル変革イニシアチブの一環として、日本のクライアント拠点（Haken導入先）で勤務できる、高度なスキルを持つバイリンガルのサイバーセキュリティ専門家を募集しています。このエンジニアは、日本の関係者と緊密に連携し、デジタルヘルスケアソリューションのための安全なインフラストラクチャクラウド環境の設計、実装、および保守を担当します。

We are looking for a highly skilled Bilingual Cyber Security Expert to work onsite at our client location in Japan (Haken deployment) for a strategic Medical Digital Transformation initiative. The engineer will work closely with Japanese stakeholders to design, implement, and maintain a secure infrastructure cloud environment for Digital Healthcare solutions.

■チーム規模 / Team Structure：
就業先オンサイトチームには、数年間就業実績のあるQuest Global社員が複数名います。
There are other Quest Global onsite members already working there in the team for many years.

■Quest Globalで働く魅力 / Why Work with Quest Global in This Domain?：

- 大手医療機器メーカーとの協業：
  -世界をリードする日本の大手企業と共に、最先端の医療機器を支える仕事
- 最先端プロジェクト：
  -AIによる欠陥検出、精密イメージング、微細パターン検査、分散コンピューティング環境などに携わるチャンス
- バイリンガル人材歓迎：
  -JLPT N2以上の日本語力を持つエンジニア、または日本語と他言語を流暢に扱えるバイリンガルエンジニアを歓迎します。グローバルな架け橋として活躍いただけます
- キャリアの成長：
  -さまざまな医療機器製造業界にわたる継続的な学習、認定、および分野横断的な機会にアクセスできます
- グローバル環境：
  -日本のオンサイトとインドのオフショアの協働で、多文化な経験とキャリア形成が可能

- Work with Major Medical Equipment Manufacturers:
  -Collaborate with leading companies in Japan that are shaping the global medical device industry
- Cutting-Edge Projects:
  -AI-driven defect detection, precision imaging, micro-pattern inspection, and distributed computing environments

- Bilingual Advantage:
  -We welcome engineers with JLPT N2 or higher Japanese proficiency, as well as professionals fluent in both Japanese and another language, who can help bridge global collaboration and deliver maximum impact
- Career Growth:
  -Access to continuous learning, certifications, and cross-domain opportunities across different medical devices manufacturing industry
- Work Environment:
  -Global collaboration between Japan onsite and India offshore teams, with cultural exchange and career enrichment

■成長機会・キャリアパス / Growth Opportunity：
このポジションでの経験を経て上位職のシニアアーキテクト、さらにはプリンシパルアーキテクトへと進むキャリアパスがあります。また、希望により営業、デリバリー、そしてQuest Globalの事業投資に大きな価値をもたらす様々なリーダーシップポジションなど、他部門や他機能における様々な役割への転身のチャンスもあります。

Excelling in this position will enable you to advance to a higher-level role as a Senior Architect and subsequently as a Principal Architect, accompanied by increased responsibilities and the possibility of a higher salary. Additionally, there may be opportunities to transition into different roles within other departments or functions, such as in Sales, Delivery, and various Leadership positions that contribute significant value to Quest Global's business investments.

【雇用形態 / Employment Type】
正社員
※試用期間あり、3ヶ月（業務・待遇変更なし）

Permanent Employee
*Trial period: 3 months, no change in duties or benefits

【給与 / Salary】
経験考慮の上、応相談（完全年俸制、1/12を毎月支給）
■残業手当：あり
■昇給：年1回（契約社員は更新のタイミングで見直しあり）

Based on experience and skill level
*Full annual salary system (1/12 paid monthly)
■Overtime allowance
■Salary increment once a year

【就業時間 / Working Hours】
会社の規定に準ずる
In accordance with company regulations

【勤務地 / Work Location】
東京都中央区晴海
Harumi, Chuo-ku, Tokyo

【休日休暇 / Vacations】

- 年間休日120日以上
- 完全週休2日制（土・日）
- 祝日
- 年末年始休暇
- 有給休暇
- 産前産後休暇
- 育児休暇
- 介護休暇
- 忌引休暇

※常駐先の業務にともなって休日・休暇は変動の可能性があります。すべて大手メーカーのため、年次休暇などは充実している場合がほとんどです。

- Total holidays: over 120 days off per year
- 2-day weekend system (Saturday and Sunday)
- National Holidays
- New Year holidays
- Paid vacation
- Prenatal and post-natal leave
- Childcare leave
- Nursing care leave
- Bereavement leave

*Holidays and vacation days may change depending on the work place you are stationed. Since they are all major manufacturers, most have generous annual vacations

【待遇・福利厚生 / Welfare】

- 通勤手当（上限2万円/月）
- 各種社会保険完備（厚生年金、健康保険 *TJK：東京都情報サービス産業健康保険組合、雇用保険、労働者災害補償保険）
- 健康診断（被扶養者健康診断、人間ドック、婦人科健診など）
- 65歳定年制 ※役職定年なし
- 社内研修制度（オンライン）

- Commuting allowance (up to 20,000/month)

- Equipped with various social insurance (Welfare pension, Health insurance *Tokyo Information Service Industry Health Insurance Association, Employment insurance, Worker's Accident Compensation Insurance)
- Health checkup (health checkup for dependents, medical checkup, gynecological checkup, etc.)
- Retirement age is 65 years old *No retirement age for positions
- Referral recruitment system (with benefits)
- In-house training system (online)

Required Skills

【必須要件/ Must Have】
※関連経験：10年以上

- サイバーセキュリティ、クラウドセキュリティ、またはエンタープライズセキュリティアーキテクチャ分野で10年以上の実務経験
- AWSクラウドプラットフォームおよびAWSセキュリティサービスに関する豊富な実務経験
- クラウドネイティブアプリケーション、API、マイクロサービス、および分散システム向けのセキュアアーキテクチャ設計経験。
- IAM、ゼロトラストアーキテクチャ、ネットワークセキュリティ、VPN、ファイアウォール、暗号化、PKI、およびセキュリティ監視に関する知識
- DevSecOps、CI/CDセキュリティ、コンテナセキュリティ、Kubernetes/EKSセキュリティ、およびInfrastructure as Code (Terraform/CloudFormation) の経験
- ISO27001、NIST、CIS、SOC2、OWASP、GDPRなどのセキュリティ標準・フレームワークに関する知識
- 脅威モデリング、脆弱性評価、ペネトレーションテスト対策支援、およびセキュリティ監査の経験
- Linux/Windowsサーバセキュリティおよびクラウドネットワークに関する深い理解
- CloudWatch、Splunk、ELK、Prometheus/Grafanaなどのログ監視ツール利用経験
- 優れた問題解決能力、コミュニケーション能力、およびステークホルダーマネジメント能力
- ビジネスレベルの英語コミュニケーション能力
- 日本顧客およびオフショア / グローバルチームと連携して業務遂行できること
- 英語：ビジネスレベル
- 日本語：JLPT N2以上

*Total and relevant experience: 10+ Year

- 10+ years of experience in cybersecurity, cloud security, or enterprise security architecture
- Strong hands-on experience with AWS cloud platform and AWS security services
- Experience designing secure architectures for cloud-native applications, APIs, microservices, and distributed systems
- Good understanding of IAM, Zero Trust Architecture, network security, VPN, firewalls, encryption, PKI, and security monitoring
- Experience with DevSecOps, CI/CD security, container security, Kubernetes/EKS security, and Infrastructure as Code (Terraform/CloudFormation)
- Knowledge of security standards and frameworks such as ISO 27001, NIST, CIS, SOC2, OWASP, and GDPR
- Experience performing threat modeling, vulnerability assessments, penetration remediation support, and security audits
- Strong understanding of Linux/Windows server security and cloud networking concepts
- Experience working with logging and monitoring tools such as CloudWatch, Splunk, ELK, or Prometheus/Grafana.
- Excellent problem-solving, communication, and stakeholder management skills
- Business-level English communication skills
- Ability to work directly with Japanese customers and offshore/global teams
- English – Business Level
- Japanese – JLPT N2 or above

【歓迎要件 / Good to Have】

- AWS Certified Security – Specialty や AWS Solutions Architect Professional などのAWS認定資格
- CISSP、CISM、CEH、CCSP、CompTIA Security+などのセキュリティ関連資格
- 医療、医療機器、半導体、または規制業界での業務経験
- HIPAA、IEC62304、ISO14971、MDR、FDAサイバーセキュリティガイドラインなどの医療系セキュリティ規格・規制に関する知識
- SIEM/SOARプラットフォームおよびインシデント対応自動化の経験
- マルチクラウドまたはハイブリッドクラウド環境 (Azure/GCP) の経験
- SAST、DAST、コンテナスキャン、およびセキュリティ自動化ツールの実務経験
- クラウドプラットフォームにおけるAI/MLセキュリティおよびデータプライバシーに関する理解
- グローバルデリバリーまたはオフショア開発モデルでの業務経験

- AWS certifications such as AWS Certified Security – Specialty or AWS Solutions Architect Professional
- Security certifications such as CISSP, CISM, CEH, CCSP, or CompTIA Security+
- Experience in healthcare, medical devices, or regulated industries
- Knowledge of healthcare cybersecurity standards and regulations such as HIPAA, IEC 62304, ISO 14971, MDR, or FDA cybersecurity guidelines
- Experience with SIEM/SOAR platforms and incident response automation
- Experience in multi-cloud or hybrid cloud environments (Azure/GCP)
- Hands-on experience with SAST, DAST, container scanning, and security automation tools
- Understanding of AI/ML security and data privacy considerations in cloud platforms
- Experience working in global delivery or offshore development models

Company Description